THAT WHICH IS CLAIMED IS:

1. A method of recovering from a failure of a primary distribution processor which provides secure communications over a network in a distributed workload environment having target hosts which are accessed through the primary distribution processor by a common network address, the method comprising the steps of:

providing to a backup distribution processor information sufficient to restart communications through the primary distribution processor utilizing network security;

detecting the failure of the primary distribution processor;

restarting the communications utilizing network security at the backup distribution processor utilizing the provided information;

routing both inbound and outbound communications with target hosts utilizing the common network address and which are associated with a secure network communication through the backup distribution processor; and

processing the inbound and outbound secure network communications at the backup distribution processor so as to provide network security processing of the inbound and outbound communications.

2. A method according to Claim 1, further comprising the step of maintaining information sufficient to restart communications through the backup distribution processor accessible to at least one distribution processor other than the backup distribution processor.

3. A method according to Claim 1, wherein the step of providing information sufficient to restart communications comprises the steps of transmitting network security information from which network security relationships associated with the communications through the primary distribution processor utilizing network security can be re-established at the backup distribution processor from the primary distribution processor to the backup distribution processor prior to failure of the primary distribution processor.

4. A method according to Claim 1, wherein the step of providing information sufficient to restart communications comprises the step of storing in a common storage accessible to the backup distribution processor, network security information from which network security relationships associated with the communications through the primary distribution processor can be re-established at the backup distribution processor.

5. A method according to Claim 4, wherein the step of restarting the communications utilizing network security at the backup distribution processor utilizing the provided information, comprises the following steps carried out by the backup distribution processor:

obtaining the network security information from the common storage;

establishing the security relationships associated with the communications through the primary distribution processor at the backup distribution processor; and

notifying target hosts associated with the communications that the backup distribution processor has taken ownership of the communications.

6. A method according to Claim 5, further comprising the step of clearing the network security information from the common storage subsequent to the backup distribution processor obtaining the network security information from the common storage.

7. A method according to Claim 5, further comprising the step of storing in the common storage, network security information from which network security relationships associated with the communications through the backup distribution processor can be re-established at another distribution processor.

8. A method according to Claim 5, further comprising the step of identifying as non-distributed communications, communications to the backup distribution processor utilizing network security which were previously distributed communications routed through the primary distribution processor.

9. A method according to Claim 5, wherein the network security comprises Internet Protocol Security (IPSec).

10. A method according to Claim 9, wherein the network security information stored in the common storage includes at least one of Phase 1 Security Association (SA) information, Phase 2 SA information and information relating the Phase 1 SA information to the Phase 2 SA information.

11. A method of recovering from a failure of a first routing communication protocol stack which routes for Internet Protocol Security (IPSec) communications between a network and a plurality of application

instances executing on a cluster of data processing systems utilizing a virtual Internet Protocol Address (VIPA) Distributor and which distributes communications for connections to at least one dynamically routable VIPA (DVIPA) to a plurality of target communication protocol stacks, the method comprising the steps of:

detecting failure of the first routing communication protocol stack at a second routing communication protocol stack;

reading ISPec information associated with the at least one DVIPA from a coupling facility of the cluster of data processing systems;

renegotiating IPSec SAs between the second routing communication protocol stack and remote IPSec peers utilizing the at least one DVIPA based on the IPSec information read from the coupling facility;

re-routing the connections to the at least one DVIPA utilizing IPSec through the second routing communication protocol stack; and

performing IPSec processing for the re-routed connections to the at least one DVIPA at the second routing communication protocol stack utilizing the renegotiated IPSec SAs.

12. A method according to Claim 11, wherein the step of renegotiating IPSec SAs comprises the steps of:

notifying an instance of an Internet Key Exchange (IKE) application associated with the second routing communication protocol stack of the failure of the first routing communication protocol stack;

providing the read IPSec information to the IKE application;

negotiating new IPSec SAs associated with the at least one DVIPA utilizing the IKE application; and

installing the new IPSec SAs in the second routing communication protocol stack.

13. A method according to Claim 12, wherein the IPSec SAs comprise Phase 1 SAs and Phase 2 SAs, the method further comprising steps of:

storing new Phase 1 SA information in the coupling facility;

storing new Phase 2 SA information in the coupling facility.

14. A method according to Claim 11, further comprising the step of clearing the IPSec information from the coupling facility after the IPSec information is read from the coupling facility.

15. A method according to Claim 11, wherein the first routing communication protocol stack carries out the steps of:

establishing IPSec SAs with remote IPSec peers utilizing the at least one DVIPA; and

storing IPSec SA information in the coupling facility sufficient to allow renegotiation of the established IPSec SAs.

16. A method according to Claim 11, wherein the IPSec SA information comprises at least one of cached Phase 1 SA policies, Phase 1 SA identifications, information correlating Phase 1 SAs and Phase 2 SAs, dynamic filter selectors and cryptographic policies.

17. A method according to Claim 16, wherein the IPSec SA information further comprises IPSec Security Parameter Indexes (SPIs) and protocols for the Phase 2 SAs.

18. A method according to Claim 17, further comprising the steps of:

installing IPSec dynamic filters in the second routing communication protocol stack; and

removing duplicates of active dynamic filters.

19. A method according to Claim 17, further comprising the step of sending a delete to an IKE associated with the first routing communication protocol stack for IPSec SAs that were active on the first routing communication protocol stack.

20. A system for recovering from a failure of a primary distribution processor which provides secure communications over a network in a distributed workload environment having target hosts which are accessed through the primary distribution processor by a common network address, comprising:

means for providing to a backup distribution processor information sufficient to restart communications through the primary distribution processor utilizing network security;

means for detecting the failure of the primary distribution processor;

means for restarting the communications utilizing network security at the backup distribution processor utilizing the provided information;

means for routing both inbound and outbound communications with target hosts utilizing the common network address and which are associated with a secure network communication through the backup distribution processor; and

means for processing the inbound and outbound secure network communications at the backup distribution

processor so as to provide network security processing of the inbound and outbound communications.

21. A system for recovering from a failure of a first routing communication protocol stack which routes for Internet Protocol Security (IPSec) communications between a network and a plurality of application instances executing on a cluster of data processing systems utilizing a virtual Internet Protocol Address (VIPA) Distributor and which distributes communications for connections to at least one dynamically routable VIPA (DVIPA) to a plurality of target communication protocol stacks, comprising:

means for detecting failure of the first routing communication protocol stack at a second routing communication protocol stack;

means for reading ISPec information associated with the at least one DVIPA from a coupling facility of the cluster of data processing systems;

means for renegotiating IPSec SAs between the second routing communication protocol stack and remote IPSec peers utilizing the at least one DVIPA based on the IPSec information read from the coupling facility;

means for re-routing the connections to the at least one DVIPA utilizing IPSec through the second routing communication protocol stack; and

means for performing IPSec processing for the re-routed connections to the at least one DVIPA at the second routing communication protocol stack utilizing the renegotiated IPSec SAs.

22. A computer program product for recovering from a failure of a primary distribution processor which provides secure communications over a network in a distributed workload environment having target hosts

which are accessed through the primary distribution processor by a common network address, comprising:

a computer readable medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which provides to a backup distribution processor information sufficient to restart communications through the primary distribution processor utilizing network security;

computer readable program code which detects the failure of the primary distribution processor;

computer readable program code which restarts the communications utilizing network security at the backup distribution processor utilizing the provided information;

computer readable program code which routes both inbound and outbound communications with target hosts utilizing the common network address and which are associated with a secure network communication through the backup distribution processor; and

computer readable program code which processes the inbound and outbound secure network communications at the backup distribution processor so as to provide network security processing of the inbound and outbound communications.

23. A computer program product for recovering from a failure of a first routing communication protocol stack which routes for Internet Protocol Security (IPSec) communications between a network and a plurality of application instances executing on a cluster of data processing systems utilizing a virtual Internet Protocol Address (VIPA) Distributor and which distributes communications for connections to at least one

dynamically routable VIPA (DVIPA) to a plurality of target communication protocol stacks, comprising:

a computer readable medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which detects failure of the first routing communication protocol stack at a second routing communication protocol stack;

computer readable program code which reads IPSec information associated with the at least one DVIPA from a coupling facility of the cluster of data processing systems;

computer readable program code which renegotiates IPSec SAs between the second routing communication protocol stack and remote IPSec peers utilizing the at least one DVIPA based on the IPSec information read from the coupling facility;

computer readable program code which re-routes the connections to the at least one DVIPA utilizing IPSec through the second routing communication protocol stack; and

computer readable program code which performs IPSec processing for the re-routed connections to the at least one DVIPA at the second routing communication protocol stack utilizing the renegotiated IPSec SAs.